Quiz 23: 4/17/15

Question 1: This code can be exploited with a buffer overflow attack. What about this code makes it vulnerable to a buffer overflow?

Question 2: What could an attacker do to the system running this vulnerable code? Assume this is a Ring3 application running as the root user.

Question 3: How could you fix the code to prevent the vulnerability?

Question 4: What are some operating system defenses to mitigate buffer overflow attacks?

```
#include <stdio.h>
int main(int argc, char **argv) {
   char buf[64];
   strcpy(buf, argv[1]);
}
```